
Вопросы теории и истории государства и права

Научная специальность

12.00.01 «Теория и история права и государства; история учений о праве и государстве»

УДК 340.12

DOI <https://doi.org/10.26516/2071-8136.2021.3.3>

ОБЩЕТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННЫХ ПРАВООТНОШЕНИЙ: ПРАВОВЫЕ РИСКИ, УГРОЗЫ И ПЕРСПЕКТИВЫ

© **Бреднева В. С., Сазанова И. В., Бакунов А. В., 2021**

Сахалинский государственный университет, г. Южно-Сахалинск, Россия

Установлено, что содержание информационных правоотношений расширяется за счет достижений научно-технического процесса и появления новых способов работы с юридической информацией. Обнаружено, что в рамках теории государства и права стала возникать необходимость формулирования общих положений и закономерностей, которые применимы для всех отраслей. Утверждается, что основными категориями, имеющими общеправовой характер, названы: информация, информационная безопасность, информационные технологии, при этом наука «теория государства и права» призвана разработать подходы к пониманию и толкованию общетеоретических категорий и их соотношению (персональные данные и право на частную жизнь; пределы использования информации о человеке и гражданине и право на предпринимательскую деятельность и др.). Сделан вывод о том, что информационные правоотношения характеризуются высоким риском наступления негативных юридических последствий. Заявлена гипотеза о потенциале информационных правоотношений менять в перспективе юридическую практику во всех отраслях. Исследована одна из таких технологий – блокчейн, юридический статус которого четко не определен. Отмечается, что информационные правоотношения нуждаются в анализе на доктринальном уровне, рекомендовано обратить внимание на новый пул проблем и угроз, для того чтобы найти универсальные способы их предотвращения, подходящие для всех отраслей права. Сделан вывод о том, что наука «теория государства и права» имеет потенциал в построении прогнозов развития государственно-правовых явлений с учетом новых технических реалий.

Ключевые слова: информационные правоотношения, информация, теория государства и права, социальная ответственность, информационные технологии, блокчейн, источники права, перспективы развития права.

Двадцать лет назад об информационных правоотношениях, информационном праве как самостоятельной отрасли ученые отзывались достаточно скептически: не было огромного количества способов обработки информации, информационные технологии в достаточно ограниченном объеме внедрялись в практическую деятельность современных компаний. В XXI в. дискуссии перешли в обратную плоскость: чем ограничивается объект информационного права. Огромное количество разносторонних явлений попало в общетеоретическую категорию «информация»: персональные данные, электронный документооборот, автоматизированные системы, облако, электронная

почта, блокчейн, криптовалюта, искусственный интеллект, электронная цифровая подпись и т. д.

В учебниках по теории государства и права информационные правоотношения практически не отражены – ни в классификациях, ни в структуре правовой системы. Тем не менее на практике выстраивалась логическая цепочка: огромные массивы информации приводили к необходимости ее упорядочивать, обрабатывать – возникающие для этого информационные технологии в процессе эксплуатации могли порождать побочные последствия – всевозможные нарушения прав физических и юридических лиц. Стали возникать вопросы о специализации юристов, о возможных стратегиях защиты нарушенных прав.

В рамках теории государства и права стала возникать необходимость формулирования общих положений и закономерностей, которые будут применимы в дальнейшем для всех отраслей. К числу таких положений можно отнести следующее:

1. Содержание информационных правоотношений базируется на применяемых информационных технологиях, расширяется за счет достижений научно-технического прогресса и появления новых способов работы с юридической информацией, носит междисциплинарный характер.

В самом общем виде информационные технологии представляют собой способы создания, обработки, передачи информации. Следует учитывать не только технический, юридический характер термина, но и социальный. Так, существуют технологии управления персоналом, которые носят информационный характер. Ярким примером является «корпоративная социальная ответственность», которая неожиданно поднимает проблему формирования источников всех информационных правоотношений.

Суть дискуссии заключается в установлении объема регулирования информационных правоотношений на локальном уровне и возможности применения не только юридических, но и социальных, этических регуляторов. Рассматривая данную технологию («корпоративная социальная ответственность»), К. Девис считал, что нельзя основываться только на минимальных требованиях закона [5, с. 313]. Точки зрения о том, что корпоративная социальная ответственность является исключительно добровольной, выходящей за рамки законодательных принуждений, придерживались также и иные авторы [4, с. 498]. Иное мнение по этому вопросу высказывал Дж. Макгуир, который еще в 1963 г. отмечал, что ответственность корпорации включает в себя не только экономические и правовые, но и дополнительные обязательства [7, с. 144].

Такой подход стал преобладающим. В отношении этических ожиданий А. Керролл отмечал, что эти требования выходят за пределы требований законодательства, но тем не менее ожидаются от бизнеса обществом (хотя и существуют сложности с определением того, что считать этическим) [4, с. 500]. Следует отметить, что дискреционными обычно называют действия, которые совершаются по личному усмотрению. В 1991 г. А. Керролл доработал свою модель, придав ей форму многоуровневой пирамиды, в основе которой лежали экономические и правовые требования.

В настоящее время стандарт ГОСТ Р ИСО 26000-2012 «Руководство по социальной ответ-

ственности» включает, среди прочего, обязанность компании соответствовать требованиям законодательства и международным нормам поведения¹.

Аналогичная ситуация характерна и для остальных правоотношений: они базируются преимущественно на требованиях законодательства. Тем не менее информационные правоотношения затрагивают вопросы персональных данных, возможности манипулирования и мотивации, выбора субъектами определенных вариантов поведения, а потому вопрос этичности полностью не закрыт.

Проблема и в том, что право отстает от жизненных реалий, от отношений, фактически складывающихся под влиянием новых технологий. Необходимо ли специальное правовое регулирование отношений или достаточно традиционных юридических конструкций? С одной стороны, при использовании информационных технологий по общему правилу действует принцип технологической нейтральности, т. е. правовое регулирование общественных отношений не зависит от характера технологии. Однако, например, популяризация информационной технологии блокчейн породила новые явления (токены, смарт-контракты), которые вызывают затруднения с точки зрения их правовой квалификации.

Кроме того, если новая технология сама позволяет решить ряд юридически значимых проблем, да еще и более эффективно, чем эти задачи решает право, то может ли это рассматриваться как основание для придания такой технологии самостоятельного правового значения [2]? На данном этапе очевидно – пробелы в правовом регулировании информационных правоотношений остаются и право не успевает за техническим прогрессом.

2. Основными категориями, имеющими общепромышленный характер, являются: информация, информационная безопасность, информационные технологии. Информационные правоотношения характеризуются высоким риском наступления негативных юридических последствий.

На практике оказалось, что декларируемая во многих нормативных актах информационная безопасность имеет немало дефектов. Например, с точки зрения российского законодательства спам (массовая рассылка) не является правонарушением, и сбор телефонными и компьютерными приложениями персональных данных вполне легализован (сам субъект, не подозревая того, при установке программы или

¹ ГОСТ Р ИСО 26000-2012. Руководство по социальной ответственности. М.: Стандартинформ, 2014. С. 2–35.

получении услуги предоставил приложению (сайту, компании) право собирать информацию о себе и направлять рекламные сообщения)¹. Так, недавно оказалось, что популярное приложение-шагомер при очередном обновлении стало запрашивать право самостоятельно совершать звонки и копировало имеющиеся в телефоне контакты. На любом устройстве можно обнаружить огромное количество приложений, которые имеют доступ к микрофону, камере, галерее фотографий, локации. Аналогичный сбор информации осуществляют различные сайты, интернет-платформы, социальные сети, причем как от самих физических лиц, так и от третьих лиц. Собираемая информация активно используется в маркетинге, например анализируются наиболее часто применяемые запросы для показа в дальнейшем пользователю таргетированной рекламы².

Немногочисленная судебная практика стала складываться не в пользу истцов, поскольку юридически либо данное действие не предусмотрено Уголовным кодексом РФ³, Кодексом РФ об административных правонарушениях⁴, либо допускается законом «О средствах массовой информации»⁵, либо сам субъект согласился с подобными условиями использования скачанных приложений, интернет-платформ⁶. В ряде случаев, даже если злонамеренные действия запрещены, то найти и привлечь к ответственности виновных лиц достаточно сложно: преступления могут совершаться с территории Пакистана, стран Африки, с использованием VPN-систем.

Распространение стал получать взлом аккаунтов в социальных сетях⁷ с параллельным взломом привязанной электронной почты с последующей просьбой у контактов помощи или займа финан-

совых средств с обещанием все вернуть. Также стали популярными взломы банковских кабинетов⁸. В качестве рекомендаций можно посоветовать также устанавливать не только пароль для входа в телефонное устройство, но и пин-код для доступа к сим-карте (для исключения вероятности, что сим-карту с украденного телефона переставят на другое устройство). Банковские кабинеты позволяют устанавливать ограничения (лимиты) на переводы и снятие денег.

Даже в зарубежной литературе признают, что достаточно сложно обеспечить информационную безопасность: организации по всему миру вкладывают огромные средства в технические средства защиты информационной безопасности, но во многих случаях не могут защитить свои информационные активы, поскольку они полагаются в основном на технические решения, которые не являются контекстно-совместимыми и достаточными. Фактически значительное количество инцидентов информационной безопасности в организации происходит из-за человеческого фактора – как преднамеренных действий, так и случайных ошибок (по версии ENISA за 2019 г. около 77 % утечек данных компаний) [6].

В этом контексте осведомленность сотрудников об информационной безопасности оказывает значительное влияние на их поведение в этой области и соблюдение ими политики безопасности. Отсутствие специальных знаний и навыков приводит к неправильному обращению с конфиденциальной информацией. Наиболее распространенной ошибкой была отправка конфиденциальных данных не тому получателю, что в основном происходило по электронной почте, по почте или факсу, а другие проблемы включали потерю или кражу документов, забывание отредактировать данные или хранение данных в незащищенном виде, например в общедоступном облачном сервере. По данным международных социологических исследований, 34 % организаций считают, что неосведомленные сотрудники являются самой большой уязвимостью, так как могут быть причиной огромных финансовых потерь и ущерба репутации предприятий [6].

Ряд основных терминов данной сферы уже получили легальное закрепление. Информация – это сведения (сообщения, данные) независимо от формы их представления. Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и ме-

¹ Определение Верховного Суда РФ от 1 нояб. 2019 г. № 302-ЭС19-20272 по делу № А69-2595/2018 // КонсультантПлюс : справочная правовая система.

² Основные положения политики конфиденциальности Samsung. URL: <https://www.samsung.com/ru/info/privacy/>; Заявление о конфиденциальности корпорации Майкрософт. URL: <https://privacy.microsoft.com/ru-ru/privacystatement>; и др.

³ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 01.07.2021) // Собр. законодательства РФ. 1996. № 25. Ст. 2954.

⁴ Кодекс Российской Федерации об административных правонарушениях от 30 дек. 2001 г. № 195-ФЗ (ред. от 01.07.2021) // Собр. законодательства РФ. 2002. № 1 (ч. 1). Ст. 1.

⁵ О средствах массовой информации : закон РФ от 27 дек. 1991 г. № 2124-1 (ред. от 30 дек. 2020 г.) // КонсультантПлюс : справочная правовая система.

⁶ Решение № 2-2794/2018 2-2794/2018-М-2357/2018 М-2357/2018 от 28 нояб. 2018 г. по делу № 2-2794/2018. URL: <https://sudact.ru/regular/doc/Fv2J1q1mJL1G/>; Решение № 2-3823/2017 2-3823/2017-М-3587/2017 М-3587/2017 от 28 сент. 2017 г. по делу № 2-3823/2017. URL: <https://sudact.ru/regular/doc/g78E1SdVR8JQ/>; Решение № 2-3795/2017 2-3795/2017-М-3588/2017 М-3588/2017 от 25 авг. 2017 г. по делу № 2-3795/2017. URL: <https://sudact.ru/regular/doc/QmxqSWcXSNWk/>; и др.

⁷ Решение № 2А-3569/2019 2А-3569/2019-М-2380/2019 М-2380/2019 от 8 мая 2019 г. по делу № 2А-3569/2019. URL: <https://sudact.ru/regular/doc/oMcihxGBfbx/>.

⁸ Приговор № 1-41/2016 1-501/2015 от 2 февр. 2016 г. по делу № 1-41/2016. URL: <https://sudact.ru/regular/doc/VKr2k6rRHcot/>.

тодов¹. Блокчейн – технология распределенно-го реестра².

Отвечая на складывающиеся угрозы, наука «теория государства и права» призвана разработать подходы к толкованию общетеоретических категорий, их соотношению (персональные данные и право на частную жизнь; пределы использования информации о человеке и гражданине и право на предпринимательскую деятельность и др.). Новым трендом должна стать техническая и юридическая возможность субъектов ограничить сбор данных о себе.

3. В перспективе изменение информационных правоотношений способно изменить юридическую практику во всех отраслях.

Например, системы распределенного реестра (блокчейн) вошли в перечень цифровых технологий, утвержденных в национальной программе «Цифровая экономика Российской Федерации»³. Реестр, построенный на блокчейн-платформе, представляет собой распределенную, без централизованного хранилища, базу данных, в которой хранится информация обо всех транзакциях участников системы в виде цепочки блоков. В такой децентрализованной базе данных хранится постоянно растущий список упорядоченных записей – блоков, каждый из которых содержит метку времени и ссылку на предыдущий блок. Новые записи могут вноситься только с согласия большинства участников системы. Транзакции верифицируются силами участников распределенного реестра. Потенциал соответствующей технологии отдельными юристами оценивается высоко. Среди преимуществ использования блокчейн-технологий называют неизменяемость информации и анонимность участников.

Информация обо всех транзакциях хранится на всех компьютерах участников обмена, что обеспечивает устойчивость к атакам и отказам оборудования. Сама суть блокчейна заключается в том, что информация, которая однажды уже была записана, не может быть изменена или удалена. Технически это возможно с помощью криптографического преобразования данных о любой транзакции. Всем заносимым в блок

транзакциям присваивается криптографический идентификатор (хеш), который добавляется в заголовок записи о следующей транзакции и так далее, в итоге хеш транзакции на вершине цепочки содержит данные обо всех предыдущих операциях, записанных в блоке [1]. Таким образом, данные об объекте и субъекте права останутся в реестре навсегда.

Организация оборота объектов гражданских прав с использованием блокчейн-технологии призвана обеспечить надежность, прозрачность транзакций. Подлог в такой системе невозможен за счет технических алгоритмов, а не за счет авторитета посредника. Более того, децентрализованный реестр позволяет осуществлять транзакции напрямую между пользователями вне зависимости от их местонахождения, исключить посредника в обмене и оплату ему комиссии, что в конечном итоге удешевляет процесс, упрощает и ускоряет передачу и обработку данных [3].

Однако принципиальные моменты архитектуры распределенного реестра данных, рассматриваемые как преимущество, создают конфликт с принципиальными положениями правовой системы.

Например, такая особенность, как неизменяемость данных системы, вступает в противоречие с правовым регулированием недействительности сделок. Недействительная сделка не порождает правовых последствий, на которые была направлена. Однако отменить запись в реестре невозможно. Последствием недействительности сделки, если субъекты приступили к ее исполнению, как правило, является реституция. Однако без активного участия другой стороны сделки провести через блокчейн возврат полученного невозможно технически. Аналогичные проблемы возникают и при отказе от исполнения договора. Если сторона договора имеет право на отказ от договора и реализует его, то каким образом может быть произведен возврат полученного по договору? Неизменяемость данных в блокчейне не позволяет осуществить подобный возврат или корректировку исполненного без содействия второй стороны.

Блокчейн ставит проблему возможности и способов принудительного исполнения. Каким образом можно арестовать, изъять имущество в системе блокчейн, если только у самого должника находятся логины и пароли, доступ к активу? Без его согласия такой доступ получить невозможно. Если сам должник добровольно не исполняет судебное решение, то проблема остается нерешенной. Более того, при осуществлении транзакции с использованием блокчейн-технологии для принятия алгоритмических решений

¹ Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ (ред. от 9 марта 2021 г.) // КонсультантПлюс : справочная правовая система.

² Об утверждении методических рекомендаций для внедрения в основные общеобразовательные программы современных цифровых технологий : распоряжение Минпросвещения России от 18 мая 2020 г. № Р-44 // КонсультантПлюс : справочная правовая система.

³ Национальная программа «Цифровая экономика Российской Федерации» : утв. Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7 // КонсультантПлюс : справочная правовая система.

на основе записей распределенного реестра высока вероятность, что узлы компьютерных сетей, участвующие в транзакции, будут локализованы в разных юрисдикциях. Соответственно, значительное количество транзакций с использованием блокчейна являются трансграничными. Трансграничный характер публичного блокчейна обостряет и проблему определения применимого права.

Публичный блокчейн дает возможность осуществлять транзакции анонимно, что вызывает определенные опасения правоохранительных органов. Лица, нарушающие закон, могут без указания личности проявлять активность в системе блокчейн, например, для легализации доходов, полученных преступным путем. Сложной является проблема ограничения доступа в блокчейн недееспособных лиц, проблема дальнейшей неопределенности субъекта юридической ответственности. Фактор неопределенности субъекта мешает традиционным подходам правового регулирования.

Еще одна серьезная проблема, связанная с распространением технологии блокчейн: создание условий деградации права на неприкосновенность частной жизни. Сведения о транзакциях, зафиксированные в публичном блокчейне, накапливаются в нем и остаются там навсегда. Это создает условия для профайлинга пользователей с применением технологии аналитики больших данных. Распределенный реестр делает принципиально невозможным использование традиционных механизмов контроля за распространением персональных данных. Действующее законодательство о персональных данных, основной идеей которого является защита фундаментальных прав человека, ориентировано на централизованные информационные системы.

Таким образом, блокчейн несовместим с идеями права и управления, поскольку живет по своим математическим законам. Именно распределенность реестра данных, являющаяся технологической сутью блокчейна, ее преимуществом, причиной популярности, противоречит принципам государственного управления и основам права.

При этом регулирующий потенциал заложен в самой технологии распределенного реестра. Блокчейн-технология сама по себе упорядочивает отношения использующих ее субъектов. Осуществление транзакций происходит по правилам, установленным протоколом платформы. В такой системе юридические средства вытесняются кардинально новым регулятором, которым становится программный код. В отличие от права информационная технология этически нейтральна. При этом ключевые параметры

программного кода разрабатываются определенными субъектами, которые и будут впоследствии их контролировать.

Однако такие саморегулируемые отношения не должны противоречить принципам права. Учитывая изложенные риски реализации отношений с помощью технологии блокчейн, можно говорить о необходимости отступления от принципа технологической нейтральности.

Справедливости ради важно отметить, что вышеописанные риски характерны для «публичных блокчейнов», в которых нет ограничений по перечню субъектов на создание блоков и на отсылку транзакций для включения в реестр, такой блокчейн не предполагает централизованного управления, наличия точек доступа. Для государственного и муниципального управления более подходит частный блокчейн, который построен на принципах централизации, ограничении возможности управления доступом, позволяя наделить полномочиями по внесению записей в реестр только специальных субъектов. Созданный на основе частного (закрытого) блокчейна, такой реестр снова создает проблемы, которые заставили юридическое сообщество обратить внимание на технологию распределенного реестра данных: такой реестр утрачивает существенную часть преимуществ публичных блокчейнов (исключение посредников, общедоступность). Содержание информационных правоотношений расширяется за счет достижений научно-технического прогресса и появления новых способов работы с юридической информацией и способно менять складывающуюся юридическую практику, в том числе судебную.

Применение информационных технологий, содержание и риски информационных правоотношений уже недостаточно изучать только в рамках отдельных блоков (например, дисциплина «Информационное право» в вузах у юристов). В настоящее время возникла необходимость разрабатывать проблематику в рамках теории государства и права, поскольку работа с информацией отражается на переосмыслении и других явлений, таких как: права человека, общество, сущность права, содержание правоприменительной деятельности. Став универсальной общетеоретической категорией, информационные правоотношения открывают новый пул проблем и угроз, которые важно доктринально изучать и искать способы их предотвращения, подходящие для всех отраслей права. Теория государства и права имеет потенциал в построении прогнозов развития государства и права в целом с учетом новых технических реалий. 

СПИСОК ЛИТЕРАТУРЫ

1. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.
2. Савельев А. И. Некоторые риски токенизации и блокчейнизации гражданско-правовых отношений // Закон. 2018. № 2. С. 36–51.
3. Сальникова А. В. Технология блокчейн как инструмент защиты авторских прав // Актуальные проблемы российского права. 2020. № 4 (113). С. 83–90.
4. Carroll A. B. A three-dimensional conceptual model of corporate performance // Academy of Management Review. 1979. N 4(4). P. 479–505.
5. Davis K. The case for and against business assumption of social responsibilities // Academy of Management Journal. 1973. N 16 (2). P. 312–322.
6. Hughes-Lartey K., Li M., Botchey F.E., Qin Z. Human factor, a critical weak point in the information security of an organization's Internet of things // Heliyon. 2021. Vol. 7, N 3. P. 1–13. <https://doi.org/10.1016/j.heliyon.2021.e06522>.
7. McGuire J. W. Business and society. N. Y. McGraw-Hill, 1963. 320 p.

REFERENCES

1. Savelyev A.I. Dogovornoye pravo 2.0: «umnyye» kontrakty kak nachalo kontsa klassicheskogo dogovornogo prava [Contract Law 2.0: “Smart” Contracts as the Beginning of the End of Classic Contract Law]. *Vestnik grazhdanskogo prava* [Bulletin of Civil Law], 2016, no. 3, pp. 32–60. (in Russian)
2. Savelyev A.I. Nekotoryye riski tokenizatsii i blokcheynizatsii grazhdansko-pravovykh otnosheniy [Some risks of tokenization and blockchain of civil law relations]. *Zakon* [Law], 2018, no. 2, pp. 36–51. (in Russian)
3. Salnikova A.V. Tekhnologiya blokcheyn kak instrument zashchity avtorskikh prav [Blockchain technology is as an instrument of copyright protection]. *Aktualnyye problemy rossiyskogo prava* [Actual problems of Russian law], 2020, no. 4 (113), pp. 83–90. (in Russian)
4. Carroll A.B. A three-dimensional conceptual model of corporate performance. *Academy of Management Review*. 1979, no. 4(4), pp. 479–505. (in English)
5. Davis K. The case for and against business assumption of social responsibilities. *Academy of Management Journal*, 1973, no. 16 (2), pp. 312–322. (in English)

6. Hughes-Lartey K., Li M., Botchey F.E., Qin Z. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*. 2021, vol. 7, no. 3, pp. 1–13. <https://doi.org/10.1016/j.heliyon.2021.e06522> (in English)

7. McGuire J.W. *Business and society*. N.Y. McGraw-Hill, 1963, 320 p. (in English)

General Theoretical Aspects of Information Legal Relations: Legal Risks, Threats and Prospects

© Bredneva V. S., Sazanova I. V., Bakunov A. V., 2021

The content of information in legal relations is expanding due to the achievements of the scientific and technical process and the emergence of new ways of working with legal information. It was found that within the framework of the theory of state and law, it became necessary to formulate general provisions and laws that are applicable to all industries. The main categories of industry-wide character are: information, information security, information technology. The science theory of state and law is designed to develop approaches to understanding and interpreting general theoretical categories and their relationship (personal data and the right to privacy; the limits of using information about a person and citizen and the right to entrepreneurial activity, etc.). It is concluded that information legal relations are characterized by a high risk of negative legal consequences. A hypothesis is stated about the potential of information legal relations to change legal practice in all sectors in the future. One of such technologies has been investigated - blockchain, the legal status of which is not clearly defined. Legal information relations need to be analyzed at the doctrinal level, it is recommended to anticipate a new pool of problems and threats in advance in order to find universal ways to prevent them, suitable for all branches of law. The science “theory of state and law” has the potential to make forecasts for the development of state and legal phenomena, taking into account new technical realities.

Keywords: information legal relations, information, legal theory, social responsibility, information technology, blockchain, sources of law, prospects for the development of law.